

11. Неприводимые многочлены. Свойства. 12. Основная теорема арифметики в кольце многочленов над полем. Каноническое разложение.

Неприводимые многочлены

Определение

Пусть $f \in K[t]$, $\deg(f) > 0$.

- Многочлен f называется **приводимым**, если $f = gh$, где $g, h \in K[t]$, $0 < \deg(g) < \deg(f)$ и $0 < \deg(h) < \deg(f)$
- Если такого разложения не существует, то f называется **неприводимым**.
- Если $f \in K[t]$ — неприводимый и $f = gh$ (где $g, h \in K[t]$), то один из многочленов g и h — константа, а другой тогда ассоциирован с f .
- Если $f \in K[t]$ — неприводимый, $f \div g$ и $0 < \deg(g)$, то $g \sim f$.

Можно провести аналогию с простыми числами. Неприводимые многочлены в некотором роде и есть простые числа.

Свойство 1

Пусть $f, g \in K[t]$, g — неприводимый. Тогда либо $f \div g$, либо $(f, g) \sim 1$.

Доказательство. • Пусть $d = (f, g)$. Тогда $g \div d$, то есть $g = dh$, $h \in K[t]$.

- Тогда либо $\deg(d) = 0$ (в этом случае $(f, g) = d \sim 1$), либо $\deg(h) = 0$.
- Если $\deg(h) = 0$, то $h \in K$ — константа и $g \sim d$.
- Так как $f \div d$ и $d \sim g$, то $f \div g$. □

Из соображений здравого смысла: два многочлена могут быть или взаимно просты, или иметь какой-то общий множитель. Но этим общим множителем может быть только неприводимый g в чистом виде, потому что g и на что не раскладывается.

Свойство 2

Пусть $g, f_1, \dots, f_n \in K[t]$ таковы, что $f_1 \dots f_n \mid g$ и g — неприводимый. Тогда существует такое $i \in \{1, \dots, n\}$, что $f_i \mid g$.

Доказательство. • Предположим противное, пусть $f_i \nmid g$ для всех $i \in \{1, \dots, n\}$. По Свойству 1 тогда $(f_i, g) \sim 1$.

• По Свойству 3 взаимно простых многочленов, тогда и $(f_1 \dots f_n, g) \sim 1$.

• Но тогда $f_1 \dots f_n \nmid g$ (в этом случае должно быть $(f_1 \dots f_n, g) \sim g$). Противоречие.

Свойство 3

Пусть $f_1, \dots, f_n, g_1, \dots, g_m \in K[t]$, причем $(f_i, g_j) \sim 1$ для всех $i \in \{1, \dots, n\}$ и $j \in \{1, \dots, m\}$. Тогда $(f_1 \dots f_n, g_1 \dots g_m) \sim 1$.

Основная теорема арифметики в кольце многочленов над полем

Теорема 5

Пусть K — поле, $f \in K[t]$, $\deg(f) \geq 1$, а c — старший коэффициент f . Тогда существует разложение $f = c \cdot p_1 \dots p_n$, где p_1, \dots, p_n — неприводимые, со старшим коэффициентом 1. Такое разложение единственно с точностью до порядка сомножителей.

Доказательство. \exists . Индукция по $\deg(f)$. **База** — случай неприводимого f . Тогда $p = c^{-1} \cdot f$ — также неприводимый, со старшим коэффициентом 1, и $f = c \cdot p$ — искомое разложение.

Переход. • Пусть для многочленов степени меньше $\deg(f)$ утверждение доказано и f — приводимый. Тогда $f = gh$, где $g, h \in K[t]$, $\deg(g) < \deg(f)$ и $\deg(h) < \deg(f)$.

• Пусть a и b — старшие коэффициенты g и h соответственно. Тогда по индукционному предположению $g = a \cdot q_1 \dots q_s$, а $h = b \cdot r_1 \dots r_\ell$, где $q_1, \dots, q_s, r_1, \dots, r_\ell \in K[t]$ — неприводимые со старшими коэффициентами 1.

• Тогда $f = c \cdot q_1 \dots q_s r_1 \dots r_\ell$ — искомое разложение для f (очевидно, $ab = c$).

! Докажем единственность индукцией по $\deg(f)$.

База: • Пусть f — неприводимый и имеет разложение $f = cp_1 \dots p_n$, где $p_1, \dots, p_n \in K[t]$ — неприводимые.

• Тогда $f = p_1g$, где $g \in K[t]$ и $\deg(p_1) > 0$. Следовательно, $f \sim p_1$, но тогда $f = cp_1$, а такое разложение ровно одно.

Переход. • Пусть единственность с точностью до перестановки доказана для многочленов степени меньше чем $\deg(f)$.


• Предположим, $f = cp_1 \dots p_n = cq_1 \dots q_m$. Тогда $q_1 \dots q_m \vdots p_1$.

• По Свойству 2 неприводимых многочленов $\exists i \in \{1, \dots, m\}$ такое, что $q_i \vdots p_1$. НУО $i = 1$.

• Так как $q_1 \vdots p_1$, q_1 неприводим и $\deg(p_1) \geq 1$, имеем $q_1 \sim p_1$. Но оба многочлена имеют старшие коэффициенты 1, следовательно, $q_1 = p_1$.

• $f = c \cdot p_1g$, где $g \in K[t]$, $\deg(g) \geq 1$ (иначе f неприводим, а этот случай разобран).

• Для многочлена g разложение на неприводимые единственно с точностью до перестановки, значит, разложения $g = p_2 \dots p_n$ и $g = q_2 \dots q_m$ могут отличаться только порядком сомножителей.

• Значит, два рассматриваемых разложения f также отличаются только порядком сомножителей. 

Определение

Каноническое разложение многочлена $f \in K[t]$ — это представление его в виде

$$f = c \cdot p_1^{k_1} \dots p_m^{k_m},$$

где c — старший коэффициент f , а p_1, \dots, p_m — различные неприводимые многочлены со старшими коэффициентами 1.

• Из ОТА следует, что каноническое разложение существует. Нужно взять разложение на неприводимые многочлены из Теоремы 5 и сгруппировать одинаковые многочлены — получится каноническое разложение.